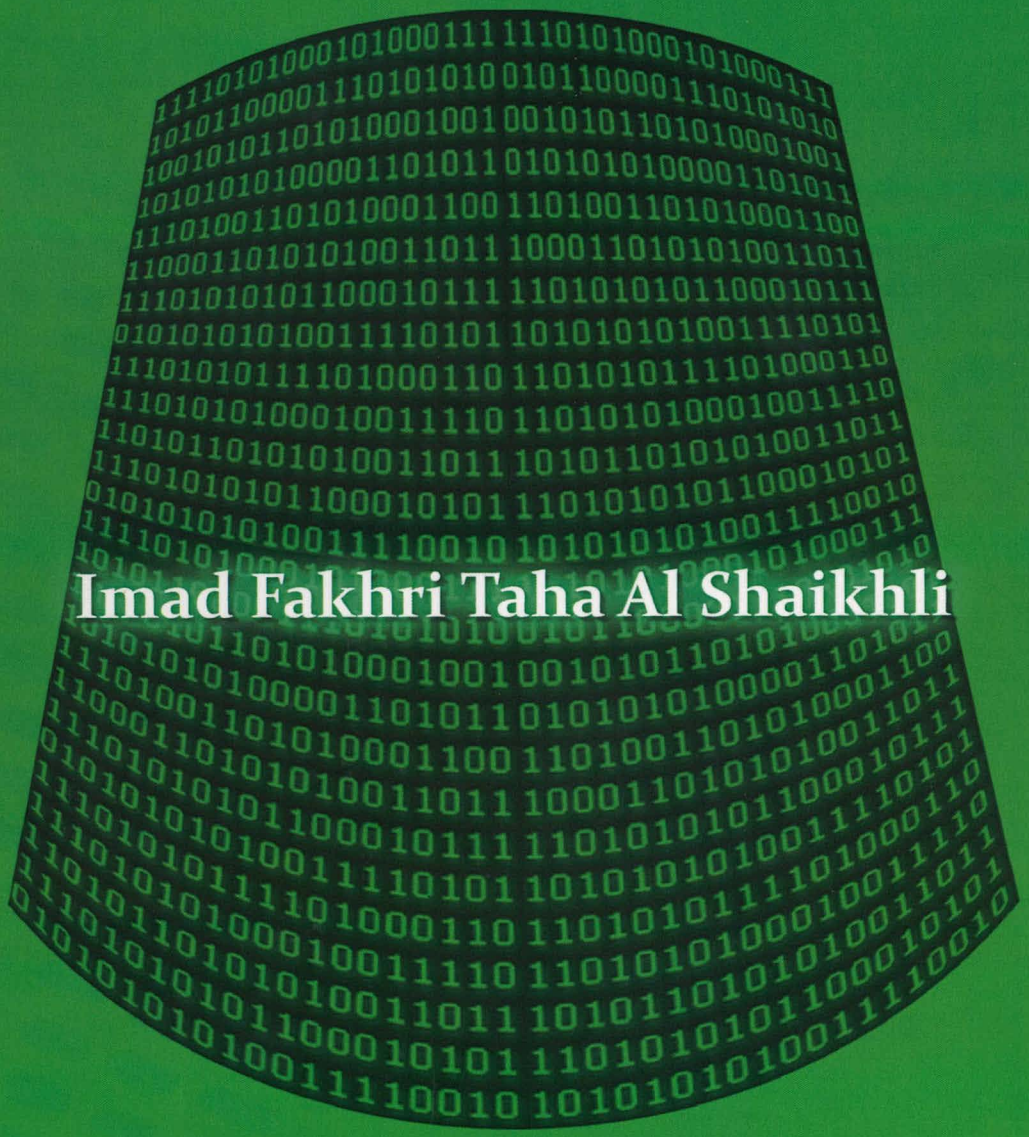
Cryptography

Past, Present and Future

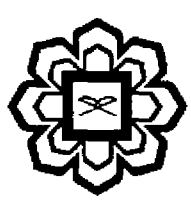


Imad Fakhri Taha Al Shaikhli

IIUM PRESS
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

Cryptography: Past, Present and Future

Imad Fakhri Taha Al Shaikhli



IIUM Press

Published by:

IIUM Press

International Islamic University Malaysia

First Edition, 2011

©IIUM Press, IIUM

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without any prior written permission of the publisher.

Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Imad Fakhri Taha Al-Shaikhli
Cryptography: Past, Present and Future
Imad Fakhri Taha Al-Shaikhli

ISBN: 978-967-418-091-1

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM
(Malaysian Scholarly Publishing Council)

Printed by :
IIUM PRINTING SDN. BHD.
No. 1, Jalan Industri Batu Caves 1/3
Taman Perindustrian Batu Caves
Batu Caves Centre Point
68100 Batu Caves
Selangor Darul Ehsan

TABLE OF CONTENTS

- Sibomana Hilali Hussein

5. Block and Stream cipher

- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Muhammad Fadil Lubis
- Usman bin Mohd Azhar
- Nopan Ziro Ando

ABSTRACT

In this article we will talk about the background of block and stream cipher and how the people were encrypt the plaintext and decrypt the cipher text using block and stream cipher. Also we will introduce into block and stream cipher individually.

BACKGROUND

Symmetric-key encryption is the method that uses same key, called secret key, for both encryption and decryption. Users exchanging data keep this key to themselves. Message encrypted with a secret key can be decrypted only with the same secret key. The algorithm used for symmetric key encryption is called secret-key algorithm. Also, secret-key algorithms are mostly used for encrypting the content of the message, so they are called content-encryption algorithms. (Blaze, M.,Diffie, W.,Rivest, R. L.,Schneier, B.,Shimomura, T., Thompson, E., &Wiener, M. (1996))

Symmetric-key encryption provides secrecy when two parties say Alice and Bob communicated. An adversary who intercepts a message should not get any significant information about its content. To set up a secure communication channel, Alice and Bob first agree on a key k. They keep their shared key k secret. Before sending a message m to Bob, Alice